Applicant thanks the Examiner for the clear statement of grounds for rejection. The Examiner's comments will be addressed by number in the following remarks.

1. Requires no response.

2. Applicant believes that the claims 21-27, as originally presented, did meet the requirement of asserting that the computer program products are embodied in a computer readable medium. However, although Applicant believes that the language suggested by the Examiner is functionally equivalent to the language first presented by the Applicant in claims 21 through 27, Applicant has changed the language of these claims to exactly correspond to the language suggested by the Examiner. Regarding the Examiner's comment that, "claims 21-27 do not positively recite that the functions are being performed by the code housed on the medium", Applicant has added the language 'performed by the codes on the computer readable medium' to each applicable recitation of function in claims 21-26. (Claim 27 does not recite a new function.)

3. Requires no response.

4. Addressing the Examiner's last comment in this section first, regarding the Examiner's assertion that Shwed discloses "the step of detecting patterns operational routine wherein a pattern of activity is detected over time (see col 6, lines 7-35)", Applicant respectfully asserts that Shwed does not attempt to detect patterns of activity in the incoming packets over time. Note that Shwed at col 6, lines 7-35 is describing a system for programming a firewall using a GUI. It does not attempt to describe the functioning of a firewall over time, nor does it at all address any patterns of activity to which the firewall may be subjected. What Shwed does describe is a process for programming the firewall wherein a series of *static* rules are programmed into the firewall. While it is apparent that this programming process does occur over time (a series of steps are sequentially performed), the question of examining incoming packets over time during the routine operation of the computer system is not addressed in this passage. Moreover, nowhere in Shwed is the detection of a pattern of activity to be detected over time. All decision operations in Shwed are based on static rules. These rules are applied, one at a time, to incoming packets "over time", but there is absolutely no mechanism for recognizing a pattern of activity.

A "pattern of activity over time" would, of course, require reference to previous packets, as each new packet is examined, since a pattern over time cannot be established by separately examining each new incoming packet without such reference. In contrast to Shwed , the present

application clearly discloses and discusses this sort of detection of patterns of activity over time. For example, at page 7 lines 26 – 29, the present application states that, "One skilled in the art will recognize that this [the 'look for known patterns' operation] will require that the INSD 10 retain certain data for a limited amount of time, as it is patterns of activity over time (as compared to a particular sequential data portion, itself) that is being examined here." This is followed by further discussion of what is meant by the detection of patterns over time, as well as several examples of such. Again, this sort of operation is simply entirely absent in the Shwed application, and is not discussed or anticipated therein in any way.

Applicant does not contest that the Shwed "gateway" is, in at least some respects, an equivalent of the term "firewall" as used in the present application, However, Applicant does respectfully suggest that the Examiner's assertion that Shwed discloses a "controller device (packet filter module)" may be the cause of some misunderstanding. Referring to Fig. 2 of Shwed, in Shwed, the "packet filters" (204) are located at the "gateways" (106 and 122) and at each "workstation" (104), having been programmed by the "packet filter generator" (208). (Note that the "packet filter generator" is, somewhat confusingly, labeled "packet filter" in Shwed Fig. 2.)

As stated at Shwed col 4, lines 33-42: The "control module" (210)

> "... enables the system administrator to keep track of the operations of the network and storage 212 can be utilized to keep logs of operations on the network and attempts of illegal entry into the network. The system operator can thereby be provided with full reports as to the operation of the network and the success or failure of the security rules. This enables the security administrator to make those changes that are appropriate in order to maintain the security of the network without limiting its connectivity."

Accordingly, please notice that the most likely comparison to the presently claimed "controller device" is the overall "workstation" (102) of Shwed. Indeed, an end user does, using the "workstation" (102) program the packet filters (using the packet filter generator), and the "workstation" (102) does monitor the operations of the network. That is, the Applicant does not contest that Shwed does disclose a "controller device", but Applicant respectfully object to the packet filters of Shwed being characterized as such.

Applicant believes that the Examiner appreciates the distinctions made above, but Applicant also recognizes the responsibility of Applicant to make the necessary distinctions clear in the claims. Accordingly, Applicant has modified claim 1 to include the limitations

of the former Claim 7, and further to include the language, "wherein .... the controller device continuously controls the firewall during the operation of the computer system. As discussed above, Shwed clearly does not do this, nor even teach in that direction. At the very most, Shwed teaches that the control device "CAN [emphasis added] be utilized to keep logs of operations on the network and attempts of illegal entry into the network." (see citation supra) Presumably, the system administrator might use this information to periodically reprogram the firewall. In Shwed, the controller clearly does NOT continuously control, the firewall, but rather does so periodically (when the system administrator uses the inventive GUI and method of Shwed to do so). A critical aspect of the present invention is that the firewall is continuously controlled by the controller, since the firewall can examine only one packet at a time for the characteristics of that packet, only a controller that is continuously controlling the firewall can send a signal to the firewall to block an incoming communication when a "pattern of activity over time" is detected by the controller.

Regarding independent claim 13, Applicant has added the language "generally simultaneously" to indicate that the controller controls the firewall "generally simultaneously" as a breach is detected – as opposed to Shwed which, as discussed above, only controls the firewall when the user chooses to add, delete or modify "rules". For the record, Applicant respectfully avers that claim 13, as modified, now contains the three major patentable distinctions of the present invention – that the controller continuously controls the firewall, that a decision can be based on an examination of a series of packets over time (rather than basing decisions on each individual packet only) and that an action can be chosen from a spectrum of potential actions based upon the gravity of a detected breach.

5. Requires no response.

6. Applicant does not, herein, specifically either contest nor agree with the Examiner's assertions, except as discussed below. Applicant believes that the dependent claims discussed are allowable as further restrictions to the allowable independent claims, whether or not the specific distinctions of independent claims which are cited by the Examiner exist in the prior art.

While Applicant is not, herein, specifically arguing against each of the Examiner's comments, Applicant does believe it necessary to make clear for the record a respectful disagreement with the Examiner's assertion: "As per claims 17, and 18. Shwed discloses the claimed method

wherein the classification of the attempted security breach includes a factor relating to the number of attempts made in the course of the attempted security breach (e.g. see col 5 lines 6-67, col 6 lines 1-35, col 7, lines 62-67, col 8 lines 1-19)." Indeed, col 5 lines 6-67 reveal the Shwed anticipates accepting or rejecting packets based on ONLY 4 (possibly 5) parameters. In Shwed, the "RULES" for accepting or rejecting packets analyze each individual packet using ONLY the paramaters 1) source, 2) destination, 3) type of service, and 4) action to be taken and possibly 5) object (gateway, terminal, etc.) on which the rule is to be enforced. (see Shwed col 5, lines 22-40.) This emphasizes TWO important distinctions between Shwed and the present invention. First, a devise based on the invention of Shwed clearly cannot base accept/reject decisions on a detected pattern of activity over time, since each packet is examined individually and accepted or rejected based solely on the "rules" installed by the user. Second, a devise based on the invention of Shwed does not assign a relative weight to an attempted breach, since the only alternatives are accept or reject. In the present claims 9 and 10, what is claimed is the assigning of a weight and the resultant selection from a spectrum of alternatives – not just accept or reject, but also, for example, reject all future communications from a sender for a preset period of time. Absolutely no such provision is anticipated by Shwed or any other prior art known to Applicant.

CONCLUSION

Claims 1 through 6 and claims 8 through 27 are now in the case. Claim 7 is canceled. Applicant's position is that the present application discloses and claims at least three major patentable distinctions over the prior art: 1) That the controller of the present invention continuously controls the firewall (based upon attempted breaches detected by the controller), 2) that the controller examines patterns of activity over time for breaches (that is, that a series of packets is examined for actions such as, for example, sequentially polling ports of the protected system) and 3) that the system can select from a spectrum of responses based only an assigned weight of a perceived breach. Applicant recognizes that the original claim 1 was defective in that it did not adequately point out any of these three distinctions, and this has been corrected by amendment herein. While Applicant believes that the independent claim 13 was distinguishable over the prior art in its original form (as argued herein), Applicant has, none the less, added language to make the distinction #1 to the claim.

Applicant has modified claims 21 through 27 according to the Examiner's suggestion and respectfully requests a reconsideration of these claims based upon the points made in this response. Applicant believes that all independent claims herein are now in condition for allowance, and that dependent claims are, therefore, allowable as further restrictions on the allowable independent claims. Such action is respectfully requested.

Applicant urges the Examiner to call Applicant's undersigned counsel should there be any remaining issues.

Respectfully submitted,

HENNEMAN & SAUNDERS

Date: 12/13/99

Larry E. Henneman, Jr.
Attorney for Applicants
Registration No. 41,063
(209) 833-8825

9 w. 8TH Street, Suite 600
Tracy, California 95376

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to the Assistant Commissioner for Patents, Washington, DC 20231 on 12/13/99, 1999.

12/13/99
Date Signed